现代物理基础丛书 33

量子计算与量子信息原理

第一卷：基本概念

Giuliano Benenti
〔意〕Giulio Casati 著
Giuliano Strini

王文阁 李保文 译

科学出版社

现代物理基础丛书 33

量子计算与量子信息原理
第一卷：基本概念

Giuliano Benenti
〔意〕Giulio Casati 著
Giuliano Strini
王文阁 李保文 译

重大科学研究计划项目(2007CB925200)资助

科 学 出 版 社
北 京

图字：01-2011-0924

内 容 简 介

本书是 Giuliano Benenti, Giulio Casati 和 Giuliano Strini 合著的 *Principles of Quantum Computation and Information I* 的中译本. 前两章简介量子力学与经典计算的基本内容, 并不需要读者事先掌握量子力学或者经典计算的知识; 后两章讨论量子计算和量子信息领域的主要成果. 本书内容深入浅出, 层次分明, 参考文献丰富, 并附有大量习题与答案.

本书可作为物理学、数学和计算机科学等学科的本科生和研究生的“量子计算与量子信息导论课”的教材. 也可供相关专业的教师和科研人员参考.

图书在版编目(CIP)数据

量子计算与量子信息原理. 第 1 卷, 基本概念/〔意〕Giuliano Benenti 等著; 王文阁, 李保文译. —北京: 科学出版社, 2011
(现代物理基础丛书 33)
ISBN 978-7-03-030453-7

I. ①量… II. ①贝… ②王… ③李… III. ①量子-计算-教材②量子论-教材 IV. ①TP387②0413

中国版本图书馆 CIP 数据核字(2011)第 040464 号

责任编辑：刘凤娟/责任校对：张小霞
责任印制：钱玉芬/封面设计：陈 敬

科 学 出 版 社出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

骏 走 印 刷 厂 印刷

科学出版社编务公司排版制作
科学出版社发行 各地新华书店经销
*
2011 年 3 月第 一 版 开本：B5 (720 × 1000)
2011 年 3 月第一次印刷 印张：13 3/4
印数：1—2 000 字数：268 000

定价：49.00 元

(如有印装质量问题，我社负责调换)

中译本序

量子信息的兴起已有近三十年的历史, 它是量子物理与信息科学相融合的新兴交叉学科, 其发展方兴未艾. 量子信息重大的潜在应用前景和其中引人入胜的深奥科学问题吸引着年青一代, 并将在21世纪科学和技术发展中占有重要的地位, 因此需要出版更多优秀的入门书籍, 以适应这个学科的发展. 虽然国际上已有不少这方面的参考书, 但是中译本并不多, 尤其是适合本科生和低年级研究生学习的中文书籍更少. Casati等所著的*Principles of Quantum Computation and Information I*, 为初涉这个研究领域的学生们提供了教材, 也为愿意学习量子计算与量子信息基本原理的读者提供了材料.

Casati教授是国际知名学者, 在量子混沌领域作出过公认的突出贡献. 他近年来致力于动力学系统的量子模拟算法方面的研究, 并取得了许多重要成果. 对动力学系统的介绍及对动力学演化与性质之量子模拟的讨论, 是此书的一大特色.

译者王文阁教授目前就职于中国科技大学, 从事量子力学基本理论等方面的研究; 李保文教授就职于新加坡国立大学, 进行热传导等多个方向的研究工作. 他们均活跃于科研第一线. 很高兴见到他们将Casati教授等的著作翻译为中文, 介绍给国内的读者. 相信初次涉足该领域或者对该领域感兴趣的读者, 可以通过阅读这本译著, 充分了解量子计算与量子信息的基本概念与原理. 此书的出版将会进一步推动相关方面的知识在国内的传播.

郭光灿

2010年5月31日于合肥

译 者 序

量子计算与量子信息, 相比于经典计算与经典信息, 在某些方面可能拥有后者无法比拟的优势. 经过人们几十年的努力, 量子计算与量子信息的基本理论框架已大体建立, 并且, 在实验上已经能够在较小量子系统中实现它们. 不过, 要实现有实际(商业)应用价值的量子计算与量子信息, 仍存在一些尚不能逾越的障碍. 其中, 最大的困难之一来源于与环境的相互作用所导致的退相干现象. 现在, 国内外的许多研究小组正致力于克服这些困难, 并取得了很大进展.

在国内外的一些著名大学, 量子计算与量子信息方面的知识已被纳入本科生与研究生的教学内容. 国外有不少涉及这一领域的各具特色的教科书, 其中包括意大利Casati教授等的这本著作. 由于合作关系, 我们对Casati教授十分了解. 作为国际物理界的知名教授, 他在量子混沌等领域做过开创性的重要工作, 对动力学系统造诣颇深. 从1998年起, 他的研究领域扩展到利用量子计算机模拟动力学系统的性质. 我们有意将他们的这部著作翻译为中文, 以飨读者. 翻译工作几年前即已开始, 然而, 由于科研等工作较繁忙, 迄今才得以完成.

原著分为两卷. 这里翻译的是第一卷, 介绍基本概念, 十分适合用作高年级本科生或者低年级研究生学习的教科书. 该著作的一个有别于其他量子计算与量子信息方面教科书的特色是对动力学模型量子模拟的讨论.

我们要感谢郭光灿院士对我们翻译工作的关心与支持, 并在百忙之中抽出时间, 为本译著作序. 我们也感谢中国科技大学的周正威教授, 他阅读了部分译稿并提出有益的建议; 同时感谢杜江峰教授对我们翻译工作的鼓励和提出的建议, 本译著的出版得到重大科学研究计划项目(2007CB925200)的资助. 在本译著的文字修改过程中, 出版社的编辑给予了很多帮助, 在此一并致谢. 希望这本书的出版能为量子计算与量子信息在国内的传播起到一定的作用.

序　言

编写本书的意图

本书将读者定位为物理学、数学和计算机科学等专业的大学生和研究生。对于那些相关专业大学毕业程度的学生而言，理解本书的内容也没有什么问题。阅读本书，并不需要事先掌握量子力学或者经典计算的知识。本书的最初两章简单介绍量子力学与经典计算的基本内容，为理解随后的章节提供了必要的条件。

本书分为两卷。在第一卷中，我们首先讲述为理解量子力学与经典计算所必需的基础知识，详述其基本原理，然后讨论量子计算和量子信息的主要结果。因此，第一卷适合于作为大学生或者研究生的量子计算与量子信息导论课的教材，讲授一个学期。对于那些在大学物理、数学和计算机科学课程方面已经获得了基本的物理学和数学知识，并且愿意学习量子计算和量子信息基本原理的读者，第一卷也适合作为一般性的学习资料。

第二卷讨论量子计算和量子信息的各个重要方面，包括理论与实验。该卷不可避免地包含更多专门且技术性的内容。为了理解这些内容，第一卷所讨论的知识是必不可少的。

重点内容

“量子计算和量子信息”是正在迅速发展的新领域。因此，如果不探究许多技术性细节，很难领会其基本概念和重要结果。本书为对该领域感兴趣的读者提供一个有用但又不过分繁杂的指南。因此，数学上的严格性不是我们最关切的。我们设法呈现一个简单而系统的论述，这样，读者在理解本书的内容时，就不需要再去查询其他教科书了。此外，我们并未试图去覆盖该领域的所有方面，而是更倾向于关注基本概念。对于刚开始涉足该领域的研究人员而言，这两卷书应该是有用的参考书。

要充分熟悉一个学科，习题解答是重要环节。本书包含大量的习题(含答案)，以作为正文的基本补充。为了充分理解本书中所讨论的主题，学生绝对有必要去尝试解决大部分的习题。

致读者

在第一次阅读时，有些内容并非必要，忽略它们的话，并不影响理解其余部分。

我们采用两种方式来突出这些内容:

(1) 标题之前有星号的小节, 包含更高深的内容, 可以作为补充材料。忽略这些部分, 对于阅读本书的其余部分而言, 不会导致更多的困难。

(2) 评注和例子被印成小字体。

致谢

我们要感谢一些同事的批评和建议。特别要提到的是Alberto Bertoni、Gabriel Carlo、Rosario Fazio、Bertrand Georgeot、Luigi Lugiato、Sandro Morasca、Simone Montangero、Massimo Palma、Saverio Pascazio、Nicoletta Sabadini、Marcos Saraceno、Stefano Serra Capizzano 和Robert Walters。他们曾阅读本书的初稿。我们也要感谢Federico Canobbio 和Sisi Chen。我们还要特别感谢Philip Ratcliffe, 他的评论和建议使本书得到了实质上的改进。当然, 以上诸位并不需要为本书所可能存在的任何缺点负责, 责任由作者自己承担。

目　录

引言与概述

量子力学对社会和技术产生了巨大的影响. 要理解这一点, 只要谈到晶体管的发明就足够了, 它或许是量子力学的无数应用中最显著的例子. 另外, 我们也很容易看到计算机对日常生活的巨大影响. 鉴于计算机的重要性, 可以说, 我们是生活在信息时代. 信息革命之所以可能发生, 要感谢晶体管的发明, 也就是说, 要感谢计算科学和量子力学的协同.

今天, 这种协同为基础科学和技术应用提供了完全崭新的机会和令人振奋的前景. 这里我们是指**量子力学可以用来处理和传递信息**.

为什么在不久的将来量子规律在计算中会变得重要? 小型化给我们提供了一个直觉的理解. 计算机电子工业随着集成电路尺寸的减小而发展. 为了提高计算能力, 也就是说, 提高计算机每秒所能够执行的浮点运算的数目, 小型化是必须的. 20世纪50年代, 真空管计算机每秒能够进行大约1000次浮点运算. 而今, 我们已经有了可以每秒执行超过百万亿次浮点运算的超级计算机. 如上所述, 计算能力的巨大发展之所以可能, 要归功于在小型化方面的进展. 经验告诉我们, 该进展可以用摩尔定律来定量描述. 该定律来自于摩尔在1965年的非凡观察: 在单个集成电路芯片上所能够放置的晶体管数目, 大约在一年半到两年内翻一番. 现在, 该指数增长还没有饱和, 摩尔定律仍然成立. 目前, 在单个集成电路芯片上所能够放置的晶体管数目大约是1亿个, 电路元件的尺寸大约是100nm. 如果将摩尔定律外推, 那么, 大约到2020年, 为储存单个比特的信息, 我们将到达原子尺寸. 在那里, 量子效应将不可避免地占支配地位.

很显然, 除了量子效应以外, 其他因素也可能导致摩尔定律失效. 首先是经济因素. 事实上, 建造那些制造芯片所需设备的费用随着时间也呈指数增长. 不论如何, 了解量子力学所规定的最基本极限是很重要的. 即使我们可以通过技术突破来克服经济障碍, 量子物理学还是给电路元件的尺寸设置了极限. 首先需要讨论的问题是将硅晶管的制作推向其物理极限, 还是发展其他可选择的器件, 如量子点、单电子晶体管, 或分子开关. 这些器件的共同特征, 是其尺寸为纳米量级, 此时量子效应至关紧要.

上面, 我们谈到的是可能代替硅晶体管的量子开关, 它们之间的连接为基于布尔逻辑的经典算法. 对于这种纳米尺度的开关而言, 量子效应仅仅是所必须考虑进来的一个不可避免的修正. 然而, 量子计算机代表了根本不同的挑战: 其目的是建

造一台基于量子逻辑的机器, 也就是说, 该机器利用量子力学的规律来进行信息处理和逻辑操作.

量子信息的计量单位是所谓的量子比特 (它是经典比特的量子对应). 一台量子计算机, 可以被看成是一个由许多量子比特所组成的系统. 物理上来讲, 一个量子比特是一个两能级系统, 如一个自旋1/2粒子的两个自旋态, 或者一个光子的水平极化和垂直极化态, 或者一个原子的基态和激发态. 量子计算机是一个拥有很多量子比特的系统, 其演化可以被控制. 一次量子计算, 就是作用于这些比特的态上的一个酉变换.

量子计算机的效率归因于典型的量子现象, 如量子态的叠加及纠缠现象. 与叠加原理有关的是内在的量子并行性. 简略而言, 量子计算机可以在单次运行中处理大量的经典输入. 另外, 这也意味着有可能有大量的输出. 量子算法的任务, 是基于量子逻辑, 并尽量利用量子力学所固有的量子并行性来突出所需的输出. 简而言之, 我们需要发展合适的量子软件, 也就是说, 有效的量子算法, 这样量子计算机才会有用.

在20世纪80年代, 费曼提出, 模拟量子系统的理想工具是基于量子逻辑的量子计算机. 他的这一想法孕育了物理学中一个非常活跃的研究领域. 同样非凡的是, 量子力学有助于解决计算机科学中的基本问题. 在1994年, Shor提出了一个量子算法, 利用它可以非常有效地解决素数因子分解问题, 也就是, 将一个可分解的整数分解为其素数因子. 这是计算机科学中的一个重要难题. 尽管还没有证明, 有人推测, 素数因子分解对于经典计算机而言是困难的. Shor算法可以有效地解决整数的分解因子问题, 相对于任何已知的经典算法而言, 它在速度上的改进是指数性的. 值得一提的是, 现有的一些密码系统. 例如, 在今天已经广泛使用的RSA, 是建立在下述假设基础之上的, 即不存在能够有效地进行素数因子分解的算法. 因此, 如果能在大规模的量子计算机上实施Shor算法, 那么, RSA密码系统将被破解. Grover证明, 量子力学也可以被用于在一个无结构的数据库中搜索一个有标记的条目. 在这一点上, 相对于经典计算机而言, 量子计算机的功效是二次方形式的.

量子计算机的另外一个令人感兴趣的方面是, 原则上而言, 它有可能避免耗散. 现在的经典计算机, 建立在不可逆的逻辑操作(门)之上, 其在本质上是耗散的. 不可逆计算所需的最小能量由下面的Landauer原理给出: 每删除一个比特的信息, 耗散到周围环境的能量至少是$k_{\mathrm{B}}T\ln 2$, 其中k_{B}是玻尔兹曼常量, T是计算机周围环境的温度. 每一个不可逆的经典门, 必须至少耗散这么多能量(事实上, 现在在经典计算机中所消耗的能量, 比该能量多一个数量级以上). 相反, 量子演化是幺正的, 因此, 量子逻辑门一定是可逆的. 至少从原理上讲, 量子计算机的运行可以没有能量损耗.

众所周知, 在经典计算机中, 利用少量的基本逻辑门, 就可以实现任意复杂的

计算. 这一点是非常重要的, 因为这样一来, 在改变问题的时候, 并不需要更改计算机的硬件. 幸运的是, 量子计算机也有此性质. 具体而言, 在量子线路模型中, 每个作用于一个多量子比特系统的酉变换, 都可以被分解成一些作用于单个量子比特及两个量子比特的门, 如CNOT门.

人们已经提出了许多不同的构造量子计算机的方案. 例如, 从NMR(核磁共振)量子处理器到冷离子阱, 从超导隧穿结线路到半导体自旋. 尽管在有些情况下, 人们已经在实验上实现了基本的量子门, 以及少量量子比特的量子算法, 但是, 要说哪一种方案最适合用来构造量子硬件还为时尚早. 对于某些问题而言, 量子计算机比经典计算机要强有力得多. 然而, 我们仍然需要用50~1000个量子比特, 以及从成千到上百万个量子门(精确的数目当然依赖于特定的量子算法), 才能够构造出使经典计算机望尘莫及的量子计算机.

实现量子计算机的技术挑战非常苛刻. 我们需要能够控制大量的量子比特的演化, 同时又能够进行大量的量子门操作. 退相干可以被认为是实现量子计算机的最大障碍. 这里, 退相干是指由于与周围环境的不可避免的相互作用所造成的、存储在量子计算机中的信息的衰减. 这种相互作用会影响量子计算机的性能, 引入计算误差. 此外, 还必须考虑量子计算机硬件中的缺陷所带来的误差. 尽管我们有量子纠错码, 但是, 成功纠错的前提是, 在退相干时间内, 量子计算机必须能够执行多次量子门操作. 这里, "多次"是指1 000~10 000, 其精确的数目依赖于错误的种类. 在复杂的多比特量子系统中, 该要求很难被满足.

这样就产生了如下问题: 是否有可能制造一台有用的量子计算机, 对于一些重要的计算问题, 它是否可以超越现有的经典计算机? 如有可能的话, 那么什么时候能做到? 除了退相干问题, 我们还要谈一下在寻找新的有效量子算法方面所遇到的困难. 我们知道, 量子计算机可以有效地解决整数因子分解问题, 但是对于下述基本问题, 尚无明确答案. 即什么样的问题可以在量子计算机上有效地计算? 量子计算机展示了一个迷人的前景, 但是, 其实际应用不大可能在未来的几年里实现. 那么, 要多久才能发展出所需的技术呢? 尽管原则上而言意想不到的技术突破总会经常发生, 要记住, 为了研发经典计算机所需的技术, 人们曾经付出过巨大的努力.

然而, 尽管如此, 第一个普通的演示性实验也是非凡的, 因为这可以用来检验量子力学的基本原理. 量子力学是一个十分有违直觉的理论. 我们至少可以期望, 量子计算的理论和实验将为我们带来对量子力学的更好理解. 而且, 这类研究可以激发对于单个量子系统(如原子、电子、光子等)控制的研究. 我们要强调, 这不仅仅是出于实验方面的好奇心, 在技术应用方面, 也是令人感兴趣的. 例如, 现在人们已经能够做出比标准的原子时钟更为精确的单离子时钟. 在某种意义上, 量子计算使得人们更有理由去努力实现对于各种不同类型单量子系统的操控.

另外一个重要的研究方向, 与信息的安全传输有关. 在此, 量子力学不仅使我

们可以进行更快的操作, 而且可以实施一些在经典意义上不可能实现的操作. 纠缠是很多量子信息实验方案的核心. 它是最引人入胜也最有违直觉的量子力学特征, 是在复合量子系统中所观测到的现象。纠缠的含义为, 对于两个明显分离开的粒子所进行的测量, 存在着非局域性的关联. 相互作用后的两个经典系统, 分别处于两个有明确定义的状态. 相反, 两个量子粒子相互作用之后, 一般而言, 它们不再可以被独立地描述. 这两个粒子之间存在一种纯量子的、不依赖于其空间距离的关联. 这就是著名的EPR佯谬, 由爱因斯坦、Podolsky 和Rosen 在1935年通过理想实验而提出. 他们证明, 如果我们接受了两个看起来很自然的原理, 即实在性和局域性原理, 那么, 量子理论将导致相互矛盾的结论. 实在性原理称, 如果我们能够很肯定地预测一个物理量的值, 那么, 这个值是与我们的观察无关的物理实在. 局域性原理则称, 如果两个系统在因果关系上是分离的, 则对其中一个系统所进行的任何测量, 不可能影响到对另外一个系统的测量结果. 换句话说, 信息不可能传播得比光速快.

1964年贝尔证明, 这种被称为局域实在论的观点, 将导致与量子力学相矛盾的贝尔不等式. Aspect等(1981)利用纠缠光子对进行了实验, 其结果明确违反贝尔不等式(数十个标准偏差), 而与量子力学的预言相当一致. Aspect的实验还显示, 人们可以利用实验来研究量子理论的那些基本而又有违直觉的内容. 最近的一些其他实验, 已经更加接近于理想的EPR方案所提的要求. 更一般而言, 归功于实验技术的发展以及实验精度的不断提高, 过去的想象实验已经变成了今日的真实实验.

贝尔不等式和Aspect实验的深刻意义远远超出了对量子力学可靠性的检验. 这些结果显示, 纠缠是一种在本质上全新的、超出经典物理范畴的资源, 并且, 纠缠态在实验上是可以操控的.

量子纠缠是很多量子通信方案的核心, 尤其重要的是*量子密集编码*和*量子隐形传态*. 利用量子密集编码, 通过对两个纠缠的量子比特中的一个进行操作, 可以传送两个比特的经典信息; 量子隐形传态, 允许将一个量子系统的态传送给另外一个在任意远的地方的系统. 在近期的基于光子对的实验中, 通过光纤连接, 可以将纠缠发送到10km以外的地方. 近来, 人们也已经演示了纠缠在远程自由空间中的传送, 其中的纠缠光子接收器远隔600m[①]. 要重点指出是, 在这么长的光学距离内所遇到的有效湍流, 与从地球到卫星之间的通信所遇到的湍流是相当的. 因此, 可以期望, 在不久的将来, 人们可以利用卫星连接在远距离接收器之间(如在洲际之间)传送纠缠.

量子力学对密码术也给出了独特的贡献. 它可以使通信双方能够发现其讯号是否被截听. 这一点在经典物理的范畴内是不可能的, 因为在经典范畴内, 原则上总可以将经典信息进行复制而不改变原始信息. 相反, 在量子力学里, 基于一些根本的原因, 测量过程一般都要扰动被测量的系统. 简单而言, 这是海森伯测不准原

① 这里的数据源自2003年原书订稿之时, 现在的传输能力已远远提高. ——译者注.

理的结果. 在量子密码术方面的实验进展, 给人以深刻印象. 根据已经演示的量子密码方案, 利用光纤, 已经可以在几十千米的距离内、以每秒几千个比特的速度运作. 更有甚者, 在几千米内的自由空间中, 量子密码术的实施也已经演示成功. 因此, 在不久的将来, 量子密码有可能将会是第一个找到商业用途的量子信息方案.

让我们引用薛定谔的话来结束我们的绪论: "我们从未单单用一个电子原子或(小)分子进行试验. 在想象实验中, 我们有时假设这么做, 但是, 这总会伴随着荒谬的结果..... 我们并不是在用单个粒子进行实验, 正如我们并不能在动物园里饲养鱼龙." 这一点绝对是值得注意的, 因为在50年之后的现在, 对于单个电子、原子与分子的实验, 已经是全世界实验室里的例行之事.

参考资料指南

在每一章的结尾, 我们给出一个简短的参考资料指南. 我们的目的是给出一般的参考文献. 这些参考资料可以引导读者对本书所讨论的主题作进一步的深入研究. 因此, 我们常常引征评述文章, 而不是原著.

对于量子信息和量子计算作一般性讨论的参考文献有Preskill (1998) 的讲稿、Gruska (1999) 的著作, 以及Nielsen 和Chuang 的专著. 导论程度的课本包括Williams 和Clearwater (1997)、Pittenger (2000) 和Hirvensalo (2001)的著作. 很有教益的讲稿有: Aharonov (2001)、Vazirani (2002) 和Mermin (2003)的讲稿. Brylinski 和Chen (2002) 的书讨论了量子计算的数学方面. Lo 等(1998)、Alber 等(2001)、Lomonaco (2002) 和Bouwmeester 等(2000) 的书汇集了一些很有趣的评述性文章, 其中, 最后一本书从实验角度来看特别有趣.

Steane (1998)以及Galindo 和Martin-Delgado (2002) 的论文是在量子计算和量子信息方面很有用的评述性文章. Ekert等(2001)的文章讨论了量子计算方面的基本概念. Bennett 和DiVincenzo (2000)的论文是一篇可读性很强的、关于量子信息和计算的评述性文章.

Cabello (2000, 2003) 提供了有关量子力学基础和量子信息基础的、超过8000余篇的参考文献(截至2003年6月).

第 1 章　经典计算导论

在讲解量子计算与量子信息之前, 有必要先了解一些计算机科学的基本概念. 本章对这些概念予以介绍. 我们首先讨论图灵机. 它是计算的一个基本模型, 将我们对算法的直觉理解予以形式化. 对于一个给定的问题, 如果存在一个算法的话, 那么, 这个算法一定可以在图灵机上运行. 然后, 我们介绍计算的线路模型. 线路模型与图灵机等价, 但是更接近于真实的计算机. 在线路模型中, 信息为线路所携带, 并且运用少量的基本逻辑门, 就可以实现任意复杂的计算. 为解决一个给定的问题, 重要的是找到最佳算法, 也就是说, 使用最少的资源(计算机内存、时间和能量)来解决该问题. 所谓计算复杂性问题, 其精神实质即在于此, 不过, 对此我们将仅简述关键概念而已. 最后, 我们研究计算所需的能量资源, 并讨论能量和信息的关系. 该关系在Landauer 和Bennet关于麦克斯韦妖佯谬问题的研究中给予了解答; 尤其是Landauer 原理给出不可逆计算所需的最小能量. 另外, 利用可逆门, 原则上可以进行没有能量损耗的任何复杂计算. 我们将简单讨论一个具体的可逆计算模型, 即所谓台球计算机模型.

1.1 图 灵 机

算法是指为解决某问题所设计的指令的集合. 例如, 在小学所学的整数加法和乘法, 即为算法. 对于任何整数, 这些算法总是给出正确结果.

图灵机在20世纪30年代由数学家阿兰·图灵所提出, 对于我们直觉中的算法概念, 它给出了准确的数学表述. 图灵机包含任意一个现代计算机所必需的基本元素, 即存储器、控制单元及读、写单元. 图灵的工作受启发于当时对于以下问题的激烈争论: 对于哪一类或几类问题, 可以找到求解它们的算法. 该争论由大卫·希尔伯特提出的一个问题而引起. 20世纪初, 大卫·希尔伯特提出了一个很深刻的问题: 是否存在这样一种算法, 它在原则上可以解决所有的数学问题. 希尔伯特当时认为这个问题的答案是肯定的, 不过, 我们将在本节看到, 希尔伯特的这一想法是错误的.

另一个紧密相关的问题是, 对于一个由一些公理和规则所定义的逻辑系统, 是否至少在原则上, 所有的命题都能够被证明或是证伪? 在20世纪初, 人们普遍认为该问题的答案是肯定的(当然, 这一问题的讨论并没有涉及以下问题, 即论证一个命题的真伪在实际上可能是极端困难的). 然而, 与这一观点相反, 哥德尔在20世纪30年

代证明了以下定理: 任何一个逻辑系统, 都存在不可判定的数学命题, 也就是说, 在该逻辑系统的公理和规则范围内, 存在不可能被证明或证伪的命题. 该定理并不排除以下可能性, 即在引入新的公理和规则, 并扩大所考虑的逻辑系统之后, 那个命题可以被证明或者证伪. 然而, 在新的系统中, 仍然可以发现新的不可判定的命题. 这样就得出了如下结论: 逻辑系统本身是不完整的. 要注意的是, 哥德尔定理也对计算机给出了限制, 即计算机不可能解决所有关于算法的问题.

图1.1给出了图灵机的主要元素. 其基本思想为, 使该机器能够像"人类计算机"那样进行计算. 虽然人的大脑只能存储有限信息, 人却可以使用无限量的纸来供其进行读写. 类似地, 图灵机包含以下3个主要元素:

(1) 磁带. 磁带的长度可为无限, 被分成很多单元. 每个单元内记一个字母a_i或是空白, 其中, a_i是一个有限长字母表$\{a_1, a_2, \cdots, a_k\}$中的一个字母. 在磁带中, 除了有限数目的单元外, 其余的单元都是空白.

(2) 控制器. 控制器可以处于有限个状态$\{s_1, s_2, \cdots, s_l, H\}$, 其中, H是一个特殊的态, 为停止态. 也就是说, 如果控制器的态变成H, 则终止计算.

(3) 读写头. 读写头处理磁带上的一个单元. 它从该单元读出、写入或擦掉这个单元上的字母, 然后, 向左或向右移动一个单元.

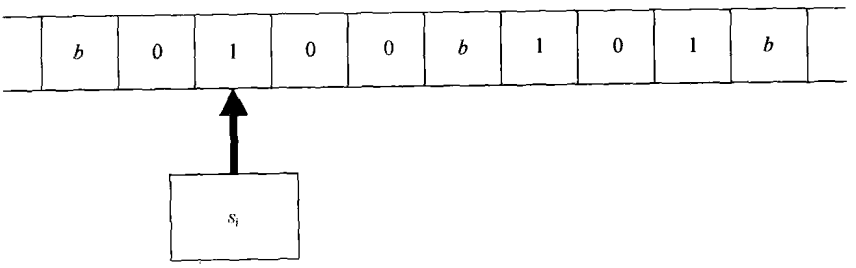

图1.1　图灵机示意图

b代表空白单元

图灵机的运作由程序控制. 这里, 程序是指一个有限的指令集合, 其中每个指令的作用, 是控制图灵机的一步运作, 并指示随后的运作. 具体而言, 指令的运作如下:

(1) 控制器由状态s变成状态$\bar{s}$;

(2) 将读写头所处理的单元的字母由a变为$\bar{a}$;

(3) 读写头左移或右移一个单元.

因此, 图灵机的一个指令由以下3个函数f_S、f_A和f_D所定义:

$$\bar{s} = f_S(s, a), \tag{1.1a}$$

$$\bar{a} = f_A(s, a), \tag{1.1b}$$